United Nations A/66/516

General Assembly

Distr.: General
14 October 2011

Original: English

Sixty-sixth session
Agenda items 134 and 146

Proposed programme budget for the biennium 2012-2013

Administrative and budgetary aspects of the financing of the United Nations peacekeeping operations

Revised estimates relating to the proposed programme budget for the biennium 2012-2013 under section 29D, Office of Central Support Services, and section 30, Office of Information and Communications Technology, related to the organizational resilience management system: emergency management framework

Report of the Secretary-General

Summary

The present report is submitted pursuant to General Assembly resolution 64/260, section II, paragraph 11, wherein the Assembly requested the Secretary-General to develop a comprehensive emergency management framework, including emergency preparedness and victim support components that would draw upon international best practices, and to submit a proposal in the context of the proposed programme budget for the biennium 2012-2013.

The present report describes a comprehensive emergency management framework based on the organizational resilience management system approach. It also describes the outcome, to date, of a pilot organizational resilience management system in the Secretariat and presents an example of its practical application in the context of the secondary data centre in Piscataway, New Jersey.

The report sets out proposed resource requirements in relation to the organizational resilience management system and a programme of work to maintain the secondary data centre, in respect of the biennium 2012-2013, under section 29D, Office of Central Support Services, and section 30, Office of Information and Communications Technology, of the proposed programme budget and under the support account for peacekeeping operations.

11-54665 (E) 251011

Please recycle

It should be noted that the present report is symbiotic with the report of the Secretary-General entitled "Enterprise information and communications technology initiatives for the United Nations Secretariat" (A/66/94), specifically the initiative entitled "Create a resilient information and communication technology infrastructure", which concentrates on the complementary technology aspects of emergency management.

I. Background

1. The varied nature of threats faced by the Organization, including critical infrastructure failures and natural hazard events, together with the vulnerability of its global operations, pose a major challenge. The need to effectively manage the impact of, and to respond to, these adverse events requires efforts beyond the crisis management, emergency response, business continuity planning and victim support efforts previously undertaken by the Secretariat and away from Headquarters and at its locations away from New York.

2. To address these challenges and pursuant to a request of the General Assembly in its resolution 64/260, a coordinated, integrated and holistic framework for emergency management, encompassing all risk-based emergency preparedness and response disciplines, is proposed in the present report. The report also seeks to respond to the recommendation of the Advisory Committee on Administrative and Budgetary Questions, endorsed by the Assembly in its resolution 65/290 on strengthening the capacity of the United Nations to manage and sustain peacekeeping operations, that the organizational resilience functions in the Departments of Peacekeeping Operations and Field Support be reviewed in the context of the report requested by the Assembly in its resolution 64/260 (sect. II, para. 11).

3. Emergency preparedness and resilience, essential elements of organizational governance, are of the utmost importance when planning and conducting activities mandated by the Secretariat at all of its locations. Recognizing this, the senior emergency policy team (see below) approved a proposal by the Crisis Operations Group to pilot an organizational resilience management system[1] approach at United Nations Headquarters as the basis for the development of a Secretariat-wide emergency management framework. In addition to harmonizing and aligning the different preparedness activities of the Organization, this framework, based on international standards and best practices, will ensure that it is better prepared to effectively respond to and recover from serious disruptive incidents.

II. Aim of the organizational resilience management system

4. The organizational resilience management system is a Secretariat initiative, based upon international best practice, to establish a comprehensive approach to the identification and management of risks related to critical disruptive events of any nature. Implementation of the system will allow the Secretariat to better prepare for and respond to disruptive events and, in many cases, preclude or inhibit those events from intensifying into emergency, crisis or disaster situations.

5. Currently, emergency preparedness efforts in the Secretariat are composed of separate planning initiatives that are led by various departments, with specialized expertise in their respective substantive areas: safety and security emergency operations (led by the Department of Safety and Security), business continuity planning, staff and victim support and medical planning (led by the Department of Management) and information technology disaster recovery planning (led by the

[1] American National Standards Institute, ASIS International SPC.1-2009 — Organizational Resilience: Security, Preparedness, and Continuity Management Systems.

Office of Information and Communications Technology). While most Secretariat locations have implemented a crisis decision-making structure that activates their different emergency preparedness plans, the Secretariat would benefit from the further elaboration of a comprehensive framework under which these initiatives can be coordinated and integrated.

6. The organizational resilience management system provides an emergency management framework that integrates emergency planning and preparedness prior to a critical event, as well as subsequent actions that address organizational crisis response, recovery, reconstitution and the return to normal business. It specifies Secretariat crisis management arrangements and brings together the emergency management aspects of the functions of business continuity, security, safety, emergency medical response, information technology disaster recovery and staff and victim support. Emergency plans associated with these functions are interlinked and mutually dependent.

7. The organizational resilience management system constitutes a "management system" approach whereby plans are developed using a systematic and coordinated process. This is in contrast to the current "silo" approach to emergency management, whereby Secretariat entities develop emergency plans that do not take into account their relationships, linkages and mutual dependencies.

8. For example, the pandemic planning exercise, which began with the threat posed by the H5N1 virus in 2005, demonstrated the benefit of emergency management plans being linked and interdependent. Such preparedness plans cannot be invoked without a crisis management structure codified in a crisis management plan. Similarly, a pandemic plan sets priorities not only for business process recovery, but also for information technology recovery. It follows then that plans must be harmonized under an integrated emergency management framework.

9. On a practical level, adopting the organizational resilience management system as a management approach would establish workflows and procedures for the common processes of individual activities, such as risk assessment, the development of risk management actions and plan maintenance, exercise and review, so that they can be conducted jointly in a coordinated way. This will result in the development and implementation of a system corresponding to a crisis environment that necessitates the simultaneous activation of the crisis response plans of multiple activities. The consequence will be a more efficient use of time and resources and improved crisis response effectiveness throughout the Secretariat.

III. Methodology for establishing and maintaining the organizational resilience management system

10. The proposed emergency management framework based on the organizational resilience management system comprises interlinked plans, with clear roles and responsibilities for decision-making and implementation, coupled with a structured maintenance, exercise and review programme. Its implementation consists of five consecutive steps: (a) policy establishment, (b) planning, (c) implementation, (d) evaluation and (e) management review.

11. As described above, the first step is to specify an organizational resilience management policy. The second step consists of a threat and risk assessment of the

natural, political, social and technological environment that could disrupt operations at a given location, the outcome of which is a prioritized list of risks with associated risk management measures that will be established and linked to a programme for action. The third step constitutes the implementation phase, which commences with the identification of roles and responsibilities within the system. Step four consists of a comprehensive evaluation of the system programme. This step will use the feedback from a maintenance, exercise and review regime as a major source of information. Step five completes the cycle with a management review.

12. Within the Secretariat, the senior emergency policy team, chaired by the Chef de Cabinet and composed of the senior leadership of most Secretariat departments, as well as high-level representatives from agencies, funds and programmes based in New York, is responsible for emergency management policy decisions. In June 2010, the senior emergency policy team approved an organizational resilience management system policy that supported the development of a pilot system focused on Headquarters in New York. Subsequently, a development group was established to develop the system as the pilot emergency management framework at Headquarters using the five-step cycle.

13. The development group conducted the planning and implementation steps of the five-step cycle, comprising the establishment of the objectives of the system, the conduct of a risk and impact assessment, the analysis of priority risks and the derivation of risk management actions from them, one of which is the maintenance of the secondary data centre (see sect. V below). The development group also assigned roles and responsibilities and developed a maintenance, exercise and review programme. The output of the planning effort was the production of a draft organizational resilience management system framework, a supporting United Nations handbook and a maintenance, evaluation and review programme for 2011-2012.

14. Upon the successful implementation of the pilot project mentioned above, the senior emergency policy team, in November 2010, reviewed and endorsed the organizational resilience management system as the emergency management framework. This endorsement validated the five-step cycle and laid the foundation for full implementation of the system throughout the global network of the Secretariat.

15. In parallel, a pilot project on the implementation of the system in field locations was conducted by the Department of Political Affairs, the Department of Peacekeeping Operations and the Department of Field Support in close coordination with the Department of Management. A training course for 22 field staff from 15 missions was conducted in April 2011. The course was presented by a joint team of the Departments of Peacekeeping Operations, Field Support and Management. While the course focused on business continuity planning, it also introduced the organizational resilience management system as the overarching emergency management framework. At the same time, the departments successfully conducted a pilot project to test business continuity methodology (including the organizational resilience management system framework) in several field missions.

IV. Roles and responsibilities

A. Overall responsibility

16. As mentioned in paragraph 12 above, the senior emergency policy team is accountable to the Secretary-General and is responsible for emergency management policy decisions. Under the organizational resilience management system, it also maintains strategic oversight over the framework within the Secretariat. The team is supported in its responsibilities in relation to the framework by the Business Continuity Management Unit in the Department of Management.

17. The Department of Management, as the lead department for the system, is responsible for developing, coordinating and integrating policy, planning, implementation and review procedures and processes and for obtaining the endorsement of the senior emergency policy team thereon. The Department of Management fulfils these responsibilities in close consultation and coordination with other Secretariat departments and, at their request, will also provide emergency preparedness planning assistance. In order to carry out its responsibilities in regard to the system, the Department of Management requires a minimum number of dedicated staff members.

18. Secretariat departments, offices, functional commissions, regional commissions and other bodies are responsible for implementing the system in their respective organizations, field presences and field operations, in accordance with policy and procedures, as approved by the senior emergency policy team. To achieve their responsibilities organizations with large field presences and operations will also require a minimum number of dedicated staff members.

B. Responsibilities of individual departments and offices

19. Recognizing that all the departments of the Organization work together in a coordinated way to achieve emergency preparedness and to bring to bear their specialized expertise, different departments have the leading role for different preparedness plans, as described below.

20. The Department of Management leads the development, coordination and integration of policy and planning procedures for the system, in close consultation with other affected departments. It is responsible for providing implementation assistance to Secretariat departments and offices in New York, as well as to offices away from Headquarters and regional commissions.

21. Upon request, the Department of Management will also provide assistance for the implementation of the system in field operations to the Department of Political Affairs, the Department of Peacekeeping Operations, the Department of Field Support and the Office for the Coordination of Humanitarian Affairs.

22. Within the Department of Management, the Business Continuity Management Unit in the Office of Central Support Services is responsible for providing guidance and hands-on support for the business continuity planning process at Headquarters, offices away from Headquarters and regional commissions. The Unit has also worked with the Departments of Political Affairs, Peacekeeping Operations and Field Support to fulfil their responsibility to introduce the required business

continuity framework and tools and to develop the required capacity to sustain business continuity in field operations.

23. The Office of Human Resources Management hosts the emergency preparedness and support team, which is dedicated to establishing human resource management mechanisms in the case of emergencies involving United Nations staff members. The role of the team is to coordinate, enable and guide the Secretariat, funds and programmes and all stakeholders prior to, during and after a crisis on all matters related to emergency preparedness and support. The team will work across the Organization at both the strategic and operational level, through best practices, lessons learned and tools, to enable each office and component involved in emergency preparedness and response to plan and work from a standard harmonized methodology. The team also serves as the communication hub for the Organization on all issues pertaining to staff, their dependants, victims and survivors of crisis situations. With respect to the emergency preparedness and support team, the Office of Human Resources Management intends to come forward with resource requests, where necessary, in the biennium 2014-2015, following a review of the workflow and activities of the team.

24. The Medical Services Division in the Office of Human Resources Management, which is responsible for providing direct medical support to Headquarters, also has a role within the organizational resilience management system framework. The Division is responsible for providing all United Nations duty stations with policy, guidance, support and training regarding public health emergencies (e.g. influenza pandemics or outbreaks of cholera) and mass casualty incidents (e.g. bombings, earthquakes and other natural disasters). This entails proactive assistance to Headquarters and other duty stations to develop, implement, maintain and test public health, emergency medical and mass casualty management plans.

25. Under the direction of the Under-Secretary-General for Safety and Security, the Department of Safety and Security oversees the security management system, including security planning and its integration into the organizational resilience management system. The Division of Headquarters Safety and Security Services provides crisis planning capabilities and is responsible for crisis management plans, security and contingency plans for Headquarters locations, offices away from Headquarters and the regional commissions.

26. As set out in the reports of the Secretary-General on the enterprise content management and customer relationship management systems and proposal for a unified disaster recovery and business continuity plan (A/64/477) and on enterprise information and communications technology initiatives for the United Nations Secretariat (A/66/94), the Office of Information and Communications Technology is to establish broad principles and develop a programme of work in which plans are set out for the resumption of critical information and communications technology services after a disruption that has had an adverse impact on key business functions of the Organization. This includes a joint effort with all units to identify critical applications that must be resilient and available in a timely fashion after a crisis.

27. Other departments work with the lead departments and offices identified above and participate in the development of overarching preparedness plans for the Organization and for their own department or office. As indicated below, departments with a field presence are responsible for preparing and executing, as

necessary, the preparedness plans for all offices, operations and/or missions falling under their direct responsibility.

C. Expansion of the organizational resilience management system to United Nations agencies, funds and programmes

28. Experience gained during the inter-agency pandemic planning and business continuity planning exercises points to the potential value of adopting a common emergency management framework with the specialized agencies, funds and programmes, based on the organizational resilience management system.

29. The necessity of integrating elements of emergency preparedness to improve resilience to adverse events and to reduce the burden on field offices by realizing economies through the integration of emergency planning exercises has also been recognized by United Nations agencies, funds and programmes. For example, the World Food Programme (WFP) is currently developing a similar approach: the WFP preparedness and response enhancement programme. The programme consists of a three-year initiative with the objective of enhancing the emergency preparedness and response capabilities of WFP, strengthening the links between headquarters and the field and enabling increasing levels of response and accountability. Under this programme, emergency preparedness and response planning will be enhanced, including the sustainable integration of risk management processes — security, operational risk management and business continuity — through the roll-out of an integrated emergency preparedness and response package.

30. The Secretary-General proposes to submit to the General Assembly at its sixty-seventh session a follow-up report summarizing the progress made in the implementation of the organizational resilience management system in the Secretariat and introducing a more comprehensive framework, including for United Nations agencies, funds and programmes. In addition, in accordance with the provisions of General Assembly resolution 64/260 related to the emergency preparedness and support team, in the context of the comprehensive emergency management framework, the team will develop the emergency preparedness and victim support components, drawing on international best practices.

V. Practical application

31. A key benefit of the organizational resilience management system approach is integration, which is a fundamental feature underlying the emergency management framework. As part of the organizational resilience management framework pilot scheme, the Secretariat crisis management structure has endorsed the risk assessment produced by the development group, which is drawn from the key Secretariat departments and offices having emergency management responsibilities and from other United Nations agencies based in New York. By virtue of the interdepartmental and inter-agency composition of the group, risk management actions reflect the interests of the United Nations at large.

32. Two practical examples of this approach are the continued maintenance of the secondary data centre in Piscataway, New Jersey, and the proposed procurement of specialized software needed for the ongoing maintenance of the different emergency

preparedness plans that fall under the organizational resilience management system framework. Both of these requirements have been identified as key management actions.

A. Secondary data centre

Establishment of the centre in Piscataway

33. In its resolution 63/269, the General Assembly approved the proposal of the Secretary-General, contained in his report on information and communications technology, disaster recovery and business continuity for the United Nations (A/63/743), to establish a new secondary data centre for United Nations Headquarters to replace the existing centre in the DC2 Building in New York. It was recognized that while the primary data centre was being relocated from the Secretariat building to the basement of the North Lawn Building, there would be a risk of information system failure. In order to mitigate that risk, a new secondary data centre would be created during the transitional period. As subsequently reported by the Secretary-General in his report on a proposal for risk mitigation measures to protect data and the information and communications systems of the Secretariat during construction work of the capital master plan (A/64/346/Add.1), the Secretariat identified a suitable data centre facility in Piscataway, New Jersey, and entered into a 30-month lease, commencing on 1 July 2009 (with an option to renew, if necessary, for an additional 30 months). In its resolution 64/228, the General Assembly requested the Secretary-General to continue to take advantage of the current economic climate in order to negotiate the most cost-effective lease and services possible and to report thereon to the Assembly at its sixty-fifth session.

34. Design of the facility was started in the first week of July 2009 and construction began in early August 2009. Construction was completed in the fourth quarter of 2009 and the facility became fully operational shortly thereafter. As reported in the eighth annual progress report on the implementation of the capital master plan (A/65/511), the secondary data centre was completed on time and ensured uninterrupted service for systems that were relocated during the period of the primary data centre migration, thus mitigating risks associated with the move. The capital master plan migration process, to which the secondary data centre was a key contributor, was completed on 15 October 2010.

Broadening the purpose of the secondary data centre to include support for the organizational resilience management system

35. Since October 2010, the secondary data centre has continued to operate as a replacement for the disaster recovery facility in the DC2 Building, which was in service for many years. At present, the secondary data centre is hosting enterprise-critical systems; however, it would be more cost-effective to integrate enterprise-critical applications, such as Umoja, i-Need, Inspira, e-mail and the Integrated Management Information System, into the enterprise data centres. Hence, the Secretary-General, in his report on enterprise information and communications

technology initiatives for the Secretariat (A/66/94),[2] proposes to migrate all enterprise-critical systems to the enterprise data centres, which will lessen the requirements on the secondary data centre to provide resilience for Headquarters, as well as other duty stations. It is expected that as the organizational resilience management system is further implemented, other enterprise-critical systems will be identified (in a collaborative exercise among departments and offices, the Business Continuity Management Unit and the Office of Information and Communications Technology), which will further reduce the requirements for the secondary data centre and correspondingly other local data centres within the Secretariat.

36. Going forward, the secondary data centre will need to remain in service to support site-specific applications and to support organizational resilience at Headquarters. Should the Assembly approve the proposal of the Secretary-General for the enterprise data centres, it is estimated that it will take two years to migrate the current list of enterprise-critical applications. Thereafter, it will be possible to reduce the size and cost of the secondary data centre.

37. In its report on information and communications technology security, disaster recovery and business continuity for the United Nations (A/63/774), specifically paragraphs 7, 8, 13, 14, 20 and 21, the Advisory Committee on Administrative and Budgetary Questions raised a number of matters regarding the establishment of the secondary data centre. These are addressed in annexes I and II to the present report.

Status of the secondary data centre

38. Funding for the establishment of the secondary data centre and its operation through to 2011 were provided jointly under the budget of the capital master plan and the support account for peacekeeping operations. An overview of actual and projected expenditure against approved funding for the implementation of the centre is provided in tables 1 to 3 below.

[2] See paras. 121, 122 and 123 (d). The enterprise data centre proposal comprises two data centres: the primary one is at the United Nations Logistics Base at Brindsi, Italy, whose function is to host enterprise-critical systems for duty stations worldwide, and the secondary centre is at the United Nations Support Base in Valencia, Spain, which serves as a backup system to provide organizational resilience.

Table 1
Expenditure for the biennium 2008-2009 against approved funding from the capital master plan
(Thousands of United States dollars)

Object of expenditure	*Approved*[a] *(a)*	*Expenditure (b)*	*Unexpended balance (c)=(a)–(b)*
1. Non-recurrent expenditures			
Contractual services	1 273.7	1 115.8	157.8
Furniture and equipment			
Data centre equipment	1 823.8	1 860.0	(36.2)
Subtotal	**3 097.5**	**2 975.8**	**121.6**
2. Recurrent expenditures			
General operating expenses			
Lease of data centre facility	1 515.2	1 467.4	47.8
Furniture and equipment			
Data centre equipment maintenance and lease	484.2	403.0	81.2
Subtotal	**1 999.4**	**1 870.4**	**129.0**
Total	**5 096.9**	**4 846.2**	**250.6**

[a] General Assembly resolution 63/269; see also A/64/346/Add.1.

Table 2
Projected expenditure for the biennium 2010-2011 against approved funding from the capital master plan
(Thousands of United States dollars)

Object of expenditure	*Approved*[a] *2010-2011 (a)*	*Expenditure 2010 (b)*	*Forecast 2011 (c)*	*Unexpended balance (d)=(a)–(b)–(c)*
General operating expenses				
Lease of data centre facility	2 261.6	1 130.8	1 130.8	—
Contractual services				
Data centre services (other contractors)	1 713.4	1 009.7	548.9	154.8
Furniture and equipment				
Data centre equipment acquisition and maintenance	5 428.3	1 976.5	3 323.8	128.0
Communication				
Telecommunication	2 193.5	—	2 193.5	—
Construction				
Alterations and improvements	47.7	36.6	—	11.1
Total	**11 644.5**	**4 153.6**	**7 197.0**	**293.9**

[a] General Assembly resolution 64/228.

Table 3

Actual and projected expenditure to 30 June 2012 against approved funding from the support account for peacekeeping operations

(Thousands of United States dollars)

Object of expenditure	*Approved 2009/10*	*Expenditure 2009/10*	*Approved 2010/11*	*Expenditure 2010/11*	*Approved 2011/12*	*Forecast 2011/12*
1. Non-recurrent expenditures						
Contractual services						
Commissioning equipment	301.4	1 254.3	—	—	—	—
Migrating applications	109.7	—	—	—	—	—
Furniture and equipment						
Data centre equipment	430.6	—	—	—	—	—
Travel	100.0	92.2	—	—	—	—
Subtotal	**941.7**	**1 346.5**	**—**	**—**	**—**	**—**
2. Recurrent expenditures						
General operating expenses						
Lease of data centre facility	687.7	676.3	401.4	401.4	326.3	212.8
Contractual services						
Data centre services (other contractors)	—	—	298.4	282.1	143.8	137.2
Furniture and equipment						
Data centre equipment maintenance and lease	402.4	—	554.4	533.9	471.5	456.3
Communication						
Telecommunication	—	—	—	—	—	92.7
Subtotal	**1 090.1**	**676.3**	**1 254.2**	**1 217.4**	**941.6**	**899.0**
Total	**2 031.8**	**2 022.8**	**1 254.2**	**1 217.4**	**941.6**	**899.0**

Future requirements for the secondary data centre

39. In his report on the status of the information and communications technology strategy for the United Nations Secretariat (A/65/491), the Secretary-General requested approval to enter into the optional lease extension for the site of the secondary data centre, which was recommended by the Advisory Committee on Administrative and Budgetary Questions in its report on information and communications technology (A/65/576) and subsequently endorsed by the Assembly in its resolution 65/259.

40. The lease is for 2,400 ft^2 of data centre space and an additional 1,569 ft^2 of office space that is currently being used as a network operations centre for the secondary data centre.

41. *The lease cost associated with the data centre* is inclusive of the provision of all data centre support infrastructure (emergency power distribution and computer room air-conditioning systems) and the cost associated with its operation and

maintenance. The United Nations is responsible for the cost of electricity and diesel fuel, based on monthly consumption.

42. The overall financial requirements for the secondary data centre facility over the course of 30 months, from 1 January 2012 to 30 June 2014, are shown below in table 4.

Table 4
Projected resource requirements under the regular budget and from the support account for peacekeeping operations
(Thousands of United States dollars)

	Regular budget		*Peacekeeping budget*[a]			
Object of expenditure	*2012-2013*	*2014-2015*	*2011/12*	*2012/13*	*2013/14*	*Total*
Recurrent expenditures						
Contractual services						
Data centre services (other contractors)	—	—	137.2	—	—	137.2
General operating expenses						
Lease of data centre facility and utilities	1 767.6	458.3	212.8	220.9	229.2	2 888.8
Data centre equipment maintenance and lease	388.8	97.2	456.3	48.6	48.6	1 039.5
Communications	741.9	185.5	92.7	92.7	92.7	1 205.5
Total	**2 898.3**	**741.0**	**899.0**	**362.2**	**370.5**	**5 271.0**

[a] 1 July-30 June.

43. The recurrent biennial operational costs for the secondary data centre will include:

(a) A provision of $137,200 as foreseen under contractual services for data centre services;

(b) A provision of $2,888,800 to cover the requirements under general operating expenses, which include the secondary data centre facility lease for 30 months covering the period 1 January 2012 to 30 June 2014 ($2,348,200) and the cost of electricity for power and cooling ($540,600);

(c) A provision of $1,039,500 to cover the maintenance and support of the servers and network equipment in the centre, including the lease payments for storage;

(d) A provision of $1,205,500 for telecommunication costs to cover Internet ($273,200) and gigabyte Ethernet ($274,500) connections, Fibre Channel cables ($390,700) and synchronous optical networking ($267,100 base cost) to provide high-speed links to the centre.

44. It is proposed that the current cost-sharing arrangement for the centre, whereby 20 per cent of the costs are met from the peacekeeping support account and 80 per cent from the regular budget, be continued, on the basis of the proportion of capacity

in the Headquarters data centre used for peacekeeping and non-peacekeeping operations.

B. Software for maintenance of emergency preparedness plans and the staff accounting system

45. As described above, the organizational resilience management system framework encompasses all the different emergency preparedness plans of the Secretariat. It also identifies links and common activities that can be undertaken in a joint fashion within the framework. Two such activities are: (a) the implementation of a system to account for all staff based in New York in a crisis, identified as a requirement in the "lessons learned" review of the Haiti crisis response and from recent events in North Africa; and (b) the automated maintenance of essential information contained in the different preparedness plans.

46. The Department of Safety and Security maintains an emergency notification system for a limited number of staff, but the Organization generally relies on broadcast e-mail, an automated message on a staff information hotline and a static website to transmit crisis information to staff. These tools do not allow the Organization to effectively communicate with all staff during a crisis event and track their status. If a crisis occurs outside office hours, staff members will often not read their e-mail and may not receive important information. It is therefore crucial for reasons of safety and security to be able to contact all staff using the suite of telecommunication devices available, including personal mobile phones and e-mail. While a global solution is being considered, under the leadership of the Department of Safety and Security with the Business Continuity Management Unit, it is recommended that the current emergency staff notification system be expanded to allow for the concurrent notification in a crisis of all staff based in New York.

47. To ensure that the emergency notification system functions properly, it is necessary to conduct tests every two to three months by sending out test messages to all the available staff telecommunication devices. These tests involve costs, which are set out in table 5 below.

48. Common components of preparedness plans, such as maintenance of staff contact data and maintenance of information on the critical infrastructure of the Organization (business processes, information technology systems, documents, etc.), have to be continuously updated, requiring a lot of effort without an automated system.

49. To address this issue, it is proposed that the Organization, under the leadership of the Business Continuity Management Unit, procure specialized software that will allow for automated maintenance of all the information contained in preparedness plans, thereby avoiding time-intensive manual updating and duplication of the same information in different plan documents.

Resource requirements for software to maintain emergency preparedness plans and the staff accounting system

50. The resource requirements, summarized in table 5 below, under the regular budget for the biennium 2012-2013 for the procurement of software for the maintenance of emergency preparedness plans and the cost of expansion of the

existing staff accounting system are estimated as follows: (a) under furniture and equipment, a one-time provision of $95,000 for the procurement of software that will allow for the maintenance of emergency preparedness plans; (b) under contractual services, a one-time provision of $68,000 for the cost of expansion of the current emergency notification system; (c) a recurrent provision of $20,000 for the biennial maintenance fee for software for the emergency preparedness plans; and (d) a provision of $60,000 for the cost of regularly conducting tests of the emergency notification system.

Table 5

Regular budget resource requirements for software, 2012-2013

(Thousands of United States dollars)

Object of expenditure	
1. Non-recurrent expenditure	
Furniture and equipment	
Software to maintain emergency preparedness plans	95.0
Contractual services	
Maintenance fee for expansion of the emergency notification system	68.0
2. Recurrent expenditure	
Contractual services	
Biennial maintenance fee for software to maintain emergency preparedness plans	20.0
Testing of the emergency notification system	60.0
Total	**243.0**

VI. Request for the establishment of posts for business continuity in the Department of Management, the Department of Peacekeeping Operations and the Department of Field Support

51. The three temporary positions of the Business Continuity Management Unit (1 P-5, 1 P-4 and 1 General Service) have been funded through general temporary assistance since September 2007. The positions were originally established to take on the work of the New York pandemic coordinator, as indicated in the report of the Secretary-General on revised estimates relating to the proposed programme budget for the biennium 2008-2009 to ensure operational preparedness and business continuity in a protracted human influenza pandemic crisis (A/62/328), and to ensure implementation of business continuity at Headquarters, offices away from Headquarters and regional commissions.

52. As a result, a business continuity planning methodology has been implemented in all of those duty stations. While business continuity programmes and capabilities have been established under general temporary assistance funding, it has been recognized that the effective maintenance of these programmes requires a more permanent and dedicated set-up. It is therefore proposed to convert the positions in

the Business Continuity Management Unit into established posts under the regular budget.

53. This will ensure that business continuity management will be successfully maintained and embedded in the culture of the Organization, enhancing its institutionalization and resilience. Maintaining a complex programme, such as business continuity management, is not achievable with a one-time effort, but requires continuous investment on the part of the Organization..

54. Furthermore, since its establishment, the tasks of the Business Continuity Management Unit have been extended. As described in the present report, the Unit will also take on the function of provision of support and guidance for the implementation of organizational resilience in the Organization, making a more permanent establishment of the Unit's posts even more essential. In addition, the Unit is frequently called upon to assist other entities with the implementation of business continuity, ensuring that the United Nations follows a consistent approach to business continuity and enabling it to respond in a more coherent fashion when faced with adverse events.

55. The Unit will continue to be located in the Office of Central Support Services, under the direct supervision of the Assistant Secretary-General, and will perform the same functions.

56. While the overall business continuity strategy for the Secretariat is the joint responsibility of the Business Continuity Management Unit and the Office of Information and Communications Technology, the Department of Peacekeeping Operations and the Department of Field Support have sole responsibility for implementing business continuity within their headquarters and field operations, with oversight from the Business Continuity Management Unit and the Office of Information and Communications Technology. Since July 2010, two general temporary assistance positions have been funded in the Office of the Chief of Staff, Department of Peacekeeping Operations/Department of Field Support (1 P-4 Organizational Resilience Officer and 1 General Service) to enable the departments to meet their direct responsibility for organizational resilience at Headquarters and in all field missions.

57. Through the efforts of the staff engaged against these funds, a business continuity planning methodology that takes into account the peacekeeping dimension of emergency preparedness has been developed and implemented in all Department of Peacekeeping Operations/Department of Field Support field operations, with the support of the Department of Management and in line with the established business continuity framework. The roll-out of the planning methodology has been supported by a training course for field operation business continuity planners. As is the case for the Department of Management, business continuity programmes and capabilities established under general temporary assistance funding will continue to be needed to ensure the continuous and effective maintenance of organizational resilience programmes and business continuity plans, requiring an established, dedicated staff capacity of one P-4 post and one General Service (Other level) post for the purpose.

58. The evolution and proper implementation of the organizational resilience management system will require an expansion in coordination of emergency preparedness plans, in particular within the field operations, as well as the

development and oversight of related training and exercise programmes. It is therefore proposed to convert the two positions (1 P-4 Organizational Resilience Officer and 1 General Service support staff) into established posts, effective 1 July 2012, to be funded from the support account for peacekeeping operations for the financial period from 1 July 2012 to 30 June 2013.

VII. Resource requirements

59. The Secretary-General has outlined above his proposals for a comprehensive emergency management framework based on the organizational resilience management system approach and requests the General Assembly to consider providing the following resources:

(a) With respect to the operational costs for the secondary data centre, the Secretary-General recommends that the Assembly approve resources in the amount of $2,898,300 for the operation of the centre;

(b) With respect to the software for maintenance of emergency preparedness plans and the staff accounting system, the Secretary-General recommends that the Assembly approve one-time resources for contractual services ($68,000) and acquisition of software ($95,000), as well as recurrent resources for software maintenance and testing of the system ($80,000);

(c) With respect to the three temporary positions (1 P-5, 1 P-4 and 1 General Service (Other level)) in the Business Continuity Management Unit provided from the regular budget, the Secretary-General recommends converting the three positions currently funded from general temporary assistance to established posts, effective 1 January 2012, as it has been determined that they will be required on a continuing basis. The Secretary-General also recommends a similar action for the two temporary positions (1 P-4 and 1 General Service) in the Office of the Chief of Staff, Department of Peacekeeping Operations/Department of Field Support, currently funded from general temporary assistance from the support account for peacekeeping operations, effective 1 July 2012.

60. Accordingly, should the General Assembly agree with the above proposals, additional resource requirements in the amount of $3,141,300 would be considered in accordance with the provisions governing the contingency fund in accordance with the terms of Assembly resolutions 41/213 and 42/211. In this regard, it is recalled that the Assembly, in its resolution 65/262, approved a contingency fund for the biennium 2012-2013 in the amount of $40.5 million.

VIII. Actions to be taken by the General Assembly

61. **The General Assembly is requested:**

(a) To approve the organizational resilience management system approach as the emergency management framework;

(b) To approve the total estimated cost of the extended lease of the secondary data centre in Piscataway for 30 months beyond 31 December 2011, as endorsed by the Advisory Committee on Administrative and Budgetary Questions in its report on information and communications technology

(A/65/576), pending the further work required before the implementation of the proposed plan;

(c) To approve the conversion of the three existing general temporary assistance positions in the Business Continuity Management Unit to established posts under section 29D, Office of Central Support Services, of the proposed programme budget for the biennium 2012-2013;

(d) To appropriate a total amount of $3,141,300 under the proposed programme budget for the biennium 2012-2013, comprising increases under section 29D, Office of Central Support Services ($243,000), and section 30, Office of Information and Communications Technology ($2,898,300), representing a charge against the contingency fund;

(e) To note that the regular budget portion of the future remaining requirements of the secondary data centre for the period from 1 January to 30 June 2014, amounting to $741,000, will be included in the proposed programme budget for the biennium 2014-2015;

(f) To approve the conversion of the two existing general temporary assistance organizational resilience positions (1 P-4 and 1 General Service (Other level)) in the Office of the Chief of Staff, Department of Peacekeeping Operations/Department of Field Support to established posts, effective 1 July 2012, to be funded from the support account for peacekeeping operations for the financial period from 1 July 2012 to 30 June 2013;

(g) To note that an amount of $941,600 under the support account for peacekeeping operations has been approved under resolution 64/228 for the financial period 1 July 2011 to 30 June 2012 for the secondary data centre;

(h) To note that future requirements for the secondary data centre in an estimated amount of $362,200 will be included in the requirements for the support account for peacekeeping operations for the financial period from 1 July 2012 to 30 June 2013 and that an estimated amount of $370,500 will be included in the requirements for the support account for the period from 1 July 2013 to 30 June 2014.

Annex I

List of current enterprise-critical systems and their resilience status

1. In paragraphs 13 and 14 of its report on information and communications technology, disaster recovery and business continuity for the United Nations (A/63/774), the Advisory Committee on Administrative and Budgetary Questions commented on the process for determining critical information technology systems.

2. In its resolution 63/262, the General Assembly requested the Secretary-General to prioritize systems in order to minimize the cost of disaster recovery and business continuity. In this respect, the Advisory Committee urged the Secretariat to make every effort to conclude this process expeditiously and to provide the Assembly with an inventory of systems classified according to their degree of criticality at the time of its consideration of this question.

3. The prioritization exercise is being undertaken by the Business Continuity Management Unit of the Office of Central Support Services as part of the business continuity planning process, and the designation of critical systems is a key outcome of this process. The determination of critical systems for United Nations Headquarters has been completed and the list of designated critical systems was included in the Secretariat business continuity plan, which was endorsed by the senior emergency policy team on 29 June 2010. Additional systems will be evaluated as appropriate.

4. The Advisory Committee was also of the view that the terminology used to qualify systems, which are referred to as critical, major, important or non-critical, merited clarification.

5. In response to the above-mentioned request of the General Assembly and the Advisory Committee's request for further clarification, a list of the critical Headquarters applications and technology systems is provided in the table below, along with information on where and how the systems are hosted and backed up within the Secretariat.

6. The table contains a list of 76 applications, which have been identified as critical (see column 1). Of those, a total of 25 applications are designated as enterprise-critical.

Enterprise-critical applications and systems (currently resilient)

7. All the applications with this designation (column 4) can be run from backup servers in the secondary data centre. This means that if the primary data centre goes offline, those applications can still operate; they are fully resilient in the secondary data centre.

Data backed up in the secondary data centre

8. The table also identifies 51 local applications that are critical, 20 of which are also backed up by the secondary data centre in Piscataway (column 2). These applications cannot be run from backup servers in the secondary data centre, but the historical information contained in the systems is safeguarded. Hence, if the primary data centre has a partial or total outage, data for the applications is not lost (e.g.

Lotus Notes e-mail, iSeek web pages). Some of the data are replicated instantly, such as Integrated Management Information System (IMIS) data, e-mail and security videos, while other data are copied nightly.

Mobile Office

9. If the primary data centre remains online but staff are required to work from home, for example in the case of a pandemic, some operations can still be accessed remotely from home, provided the staff member has Mobile Office access on his or her computer. All 25 enterprise-critical applications and 20 critical local applications are accessible via Mobile Office (column 3).

Systems designated as critical at United Nations Headquarters

Application (1)	*Data backed up in secondary data centre (2)*	*Available in Mobile Office (remote access) (3)*	*Enterprise-critical applications/systems (currently resilient) (4)*	*Department (5)*
1. IMIS 2. Lotus Notes 3. iSeek 4. Shared drives 5. Galaxy/Inspira 6. un.org 7. CORLOG database 8. Mobile Office	Y	Y	Y	Multiple departments
9. Customer relationship management, Siebel	Y	Y	Y	EOSG
10. Nucleus 11. MARS 12. FPMS 13. Videoconferencing	Y	Y	N	DFS
14. Sun system 15. CDU case files 16. SLAS roster 17. Oxford Analytical 18. CMOS database 19. PMSTAR 20. Government claims 21. Management system 22. HP Open View	N	N	N	DFS
23. Swift 24. BIS 25. OPICS 26. IMIS DIAG (diagnostic) 27. OPICS Integrated Consolidated System	Y	Y	Y	OPPBA

Application (1)	*Data backed up in secondary data centre (2)*	*Available in Mobile Office (remote access) (3)*	*Enterprise-critical applications/systems (currently resilient) (4)*	*Department (5)*
28. Nova				
29. UNICEF SAP				
30. Insight				
31. FMT				
32. Paradox	N	N	N	OPPBA
33. Invoice tracker				
34. Bloomberg Anywhere				
35. ODS	Y	Y	Y	DGACM
36. ProcurePlus				
37. ProcurePlus bid processing				
38. ProcurePlus reporting system				
39. ProcurePlus scheduling system	Y	Y	Y	OCSS/PD
40. ProcurePlus contract tracking				
41. Requisition assignment system				
42. Requisition tracking system				
43. Nova (CMP tailored)	Y	Y	N	CMP
44. Microsoft Project				
45. AutoCad	N	N	N	CMP
46. Primavera				
47. e-Meets				
48. e-Doc				
49. DTSearch	Y	Y	N	DGACM
50. Photoshop				
51. InDesign				
52. APG				
53. NICE				
54. Avanti	N	N	N	DGACM
55. Adobe CS3				
56. Kodak Prinergy EVO				
57. sqlP				
58. Trim Context 6				
59. Sabre	Y	Y	N	OCSS/FCSD
60. Vendor registration system				
61. Laissez-passer issuance and administration system	N	N	N	OCSS/FCSD
62. Various Lotus Notes databases	Y	Y	N	DPA
63. UN file transfer protocol	N	N	N	DPI
64. ProGen payroll	Y	Y	N	DPKO
65. AllPerson				

Application *(1)*	*Data backed up in secondary data centre* *(2)*	*Available in Mobile Office (remote access)* *(3)*	*Enterprise-critical applications/systems (currently resilient)* *(4)*	*Department* *(5)*
66. Human resources data warehouse	N	N	N	OHRM
67. CRM (OHRM)				
68. CMS				
69. Ez-HR				
70. Earthmed (MSD)	Y	Y	N	OHRM/MSD
71. Auto audit				
72. Case management system OIOS	N	N	N	OIOS
73. DSS website control	Y	Y	N	DSS
74. TRIP				
75. United Nations Security Management Network				
76. Security management system database	N	N	N	DSS

Abbreviations: BIS, budget information system; CDU, Conduct and Discipline Unit; CMOS, Current Military Operations Service; CMP, capital master plan project; CMS, content management system; CRM, customer relationship management; DGACM, Department for General Assembly and Conference Management; PD, Procurement Division; DFS, Department of Field Support; DPKO, Department of Peacekeeping Operations; DPA, Department of Political Affairs; DPI, Department of Public Information; DSS, Department of Safety and Security; EOSG, Executive Office of the Secretary-General; FCSD, Facilities and Commercial Services Division; FMT, funds monitoring tool; FPMS, Field Personnel Management System; MARS, Mail Action Records System; MSD, Medical Services Division; NICE, Neptune Intelligence Computer Engineering; ODS, Official Document System; OHRM, Office of Human Resources Management; OIOS, Office of Internal Oversight Services; OPICS, Operations Processing Integrated Control System; OPPBA, Office of Programme Planning, Budget and Accounts; PMSTAR, Police and Military Staff Travel and Rotation; SAP, Systems, Applications and Products in Data-Processing; SLAS, Senior Leadership Appointments Section; TRIP, travel request information processing; UNICEF, United Nations Children's Fund.

Annex II

Responses to matters raised by the Advisory Committee on Administrative and Budgetary Questions

1. In its report on information and communications technology, disaster recovery and business continuity for the United Nations (A/63/774), the Advisory Committee on Administrative and Budgetary Questions raised a number of matters, specifically in paragraphs 7, 8, 14, 20 and 21, which are set out in the table below, together with the response of the Secretary-General.

2. The Committee also commented on the process for determining critical systems in paragraphs 13 and 14, which are addressed in annex I.

Recommendation	*Response*
The Committee recommends that a final decision on whether to lease or purchase be based on an analysis of which option would result in the least cost to the Organization, taking into account the expected lifespan of the relevant ICT equipment (A/63/774, para. 7).	In deciding the location of the secondary data centre, a thorough analysis was undertaken with respect to the costs associated with either renovating the existing facility in the DC2 Building or seeking an acceptable lease for a nearby "ready" facility. A secondary data centre in Piscataway represented the best alternative, due to significant difficulties with the DC2 facility related to deficient emergency power, poor air conditioning and other factors, which made it unlikely that a retrofit would be possible within the time frames required by the capital master plan. It was imperative to meet this time frame, since there were significant potential costs related to construction delays (approximately $14 million per month) if an operational backup facility could not be completed on time. The secondary data centre was completed on time and construction delays were avoided, which demonstrates that the best alternative for the Secretariat was selected.
The Committee was informed that, due to capacity limitations in the primary data centre in the Secretariat building, [certain] non-critical departmental applications are hosted in DC2 only (ibid., para. 14).	The migration of the primary data centre to the North Lawn Building was completed in 2010 and the new facility has greater capacity, which means that the non-critical systems previously hosted in the DC2 secondary data centre are now hosted in the primary data centre facility.
The Committee emphasizes the importance of the conduct of a full analysis of costs and the provision of complete costing information to facilitate its consideration of and decision-making on such proposals, particularly in the light of the potential for duplication and the resource implications (ibid., para. 8).	The proposed organizational resilience management system framework will provide a business-led coordinated strategy which will ensure that organizational resilience is realized at the most efficient cost.

Recommendation	*Response*
The Committee further recommends that the Secretary-General be requested to review the migration strategy with a view to seeking efficiencies, prioritizing among the critical and non-critical applications to be migrated and optimizing the utilization of existing facilities, and to ensure that the scope of the project is as lean as possible, consistent with the need to preserve the integrity of the Organization's data (ibid., para. 20).	The Secretary-General presented his proposal for streamlining data centres in his report on the status of implementation of the information and communications technology strategy for the United Nations Secretariat (A/65/491), which also described estimated savings associated with the establishment of an enterprise data centre. The General Assembly requested the Secretary-General to present new and/or revised proposals (resolution 65/259) and in response the Secretary-General has set out amended proposals in his report on enterprise information and communications technology initiatives for the United Nations Secretariat (A/66/94, sect. II.D). This proposal envisages that the local data centre configuration will require facilities such as the secondary data centre to be maintained, but with a much smaller footprint and at a lower cost. It should be noted that the Headquarters secondary data centre was designed with a small footprint, with a view to later migrating the enterprise-critical systems to an enterprise data centre when ready. As elaborated upon in the above-mentioned report, the Secretary-General has fully leveraged all existing facilities to lower costs and restated the benefits related to the enterprise data centre concept. After thorough analysis, it was determined that it was less expensive and more efficient to leverage existing facilities in the United Nations Logistics Base at Brindisi, and the United Nations Support Base in Valencia. In addition, this will stem migration costs for enterprise systems, such as Umoja and others. Migration will be implemented with close consultation between departments, offices, the Business Continuity Management Unit and the Office of Information and Communications Technology. Enterprise-critical systems will be hosted in the enterprise data centre, while local unique systems will be hosted in local data centres and will be backed up in local secondary data centres. In this manner, only enterprise-critical applications will be backed up at the enterprise data centre, significantly reducing operating and disaster recovery costs to the Secretariat.

Recommendation	*Response*
The Committee recommends that the Secretary-General be requested to utilize the services of an independent expert possessing a high degree of technical experience in the field of migration and relocation of data centres to validate the project implementation plan and provide advice to the implementation team, as required, without disrupting the project schedule, to be funded from within existing resources (ibid., para. 21).	Since the report of the Committee was prepared, the Business Continuity Management Unit and the Office of Information and Communications Technology have identified the required methodologies and are currently implementing processes based on these best practice methodologies to effectively manage this ongoing need of classifying systems/applications. These methodologies and practices were used to determine the population of critical systems for Headquarters, which has now been completed. The resulting list comprises both enterprise-critical and other unique, critical local systems, and is set out in annex I to the present report.